Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 30 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Federal Deposit Insurance Corporation states in its findings on identity theft that there is a need for new safeguards for Internet banking, with new and better ways of identifying real customers from those trying to hijack bank accounts. (See item 5)
- The Christian Science Monitor reports the recent thefts of two small planes renew small airport security concerns that in this post−9/11 era the thieves could have easily been al Qaeda operatives and not teenagers out for a thrill. (See item 6)
- Government Executive reports the FBI is rolling out a Regional Data Exchange program that allows federal law enforcement agencies and state and local police forces to share information throughout local regions of the country. (See item 24)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 29, The Ottawa Citizen (Canada)* — **Ottawans asked to conserve power.** Ottawa, Canada, residents are being told to conserve electricity in an effort to keep the province's fragile power system afloat. Across Ontario demand for electricity reached 25,861 megawatts, just shy of the all−time high of 26,157 the province hit on Monday, June 27. For a second day in a row, demand exceeded supply and Ontario was forced to rely on imported power from the U.S. to

keep its system working. Councilor Peter Hume, the city's planning and environment committee chairman, said the Britannia water filtration plant had been taken off the power grid and was running on generators. He called on Ottawans to use as little water as possible. Norm Fraser, vice−president of operations for the provincial utility Hydro One, said he does not expect any brownouts or blackouts but still called for conservation to keep a cushion of power available if demand climbs even higher. The province's chief conservation officer, Peter Love, said that growth in population and the economy, he said, were behind the province's ever−higher demand for electricity. Added to that, Hydro One is in the midst of a strike by about 1,000 engineers.
Source: http://www.canada.com/nanaimo/story.html?id=eac4cb09−5348−476f−822d−6ec2fc1eb013

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

2. *June 29, Associated Press* — **India to tighten data secrecy laws.** India will tighten laws to prevent cyber crimes and ensure data secrecy after a call center employee allegedly sold personal data on 1,000 British customers, an official said Wednesday, June 29. The scandal has shaken India's booming outsourcing industry, which provides telemarketing services, call center operations, payroll accounting, and credit card processing for hundreds of Western companies. Prime Minister Manmohan Singh told representatives of India's software companies at a meeting Wednesday that laws would be tightened to prevent cyber crimes such as the illegal transfer of commercial information. Violators will be prosecuted, the prime minister's spokesperson, Sanjaya Baru, said Wednesday. Kiran Karnik, head of the National Association of Software and Service Companies, or NASSCOM, said the Indian data processing industry was committed to ensuring ``the highest standards of data privacy." NASSCOM said it is building a central database of all outsourcing industry employees to prevent criminals from getting jobs in the sector and threatening the data security of global companies.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=KZB0F0VSVEFHYQSNDBCCKH0CJUMEKJVN?articleID=164903812

3. *June 29, Vnunet.com (UK)* — **Hackers unleash industrial spy Trojan.** IT security experts have detected a malware−based hack attack that attempts to gain unauthorized access to the networks of specifically targeted domains. Security firm MessageLabs, which discovered the attack, explained that the Trojan targets only a small number of e−mail addresses rather than

mass mailing itself to as many recipients as possible. The infected e−mails were transmitted to a highly targeted list of recipients at only four domains, suggesting that the hackers were using the malware for industrial espionage. The attack is designed to exploit a vulnerability in Microsoft Word. The majority of the e−mails were bound for addresses at one particular international organization that operates in the global security arena. This is the second time that MessageLabs has intercepted attacks aimed at this organization over the past month. "The motivation behind today's new email−borne threats is far more sinister than traditional methods of large−scale attacks," said Mark Sunner, chief technology officer at MessageLabs. "New criminal methods show a preference for selecting a particular target to attack, whether an individual or an organization, for perhaps financial or competitive gain. The architects behind the bespoke Trojan attacks we are witnessing aim to steal confidential corporate information and intellectual property," said Sunner.
Source: http://www.vnunet.com/vnunet/news/2139033/hackers−unleash−in dustrial−spy

4. *June 28, Associated Press* — **IRS orders security review of ChoicePoint contract.** The Internal Revenue Service (IRS) said Tuesday, June 28, it has ordered a full security review of a $20 million contract awarded to ChoicePoint Inc., a data broker under fire for a security breach that let criminals gain access to its database of personal information. IRS Commissioner Mark Everson ordered the security review of the five−year contract to make sure it will not endanger taxpayer confidentiality, the agency said in a statement. The IRS said it had no security problems during a previous five−year contract with the company. The arrangement allows IRS auditors and criminal investigators to use ChoicePoint's databases to locate assets owned by delinquent taxpayers. It's part of an IRS effort to close a more than $300 billion gap between taxes owed and taxes paid. ChoicePoint would be given names, addresses, and Social Security numbers for data searches. Their employees would be bound by the same federal privacy laws and regulations governing IRS employees.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=KZB0F0VSVEFHYQSNDBCCKH0CJUMEKJVN?articleID=164903626

5. *June 27, Federal Deposit Insurance Corporation* — **Latest FDIC findings on identity theft suggest need for new safeguards for Internet banking.** User names and passwords should be supported in Internet banking transactions with new and better ways of identifying real customers from fraud artists trying to hijack bank accounts, according to an update on identity theft from the Federal Deposit Insurance Corporation (FDIC). "Identity theft, particularly account hijacking, continues to grow as a problem for the financial services industry and for consumers," said FDIC Chairman Don Powell. "Our review illustrates that ID theft is evolving in more complicated ways and that more can and should be done to make online banking more secure." The new findings are in a supplement to an FDIC study issued in December about ways to fight phishing scams. The supplement reviews and responds to public comments that the FDIC received about the original study, identifies the most recent trends in identity theft, and discusses a variety of new technologies that could be used to make Internet banking more secure.
Study supplement: http://www.fdic.gov/consumers/consumer/idtheftstudysupp/inde x.html
Source: http://www.fdic.gov/news/news/press/2005/pr5805.html

[Return to top]

Transportation and Border Security Sector

6. *June 29, Christian Science Monitor* — **Two thefts of small planes renew security concerns.** In the past two weeks, two small planes have been stolen and taken for joy rides. In neither case was the crime a national security threat, but some analysts note that in this post−9/11 era the thieves could have easily been al Qaeda operatives and not teenagers out for a thrill. That has again raised the question of whether enough is being done to secure the more than 19,000 small airports scattered across the nation. After 9/11, the Federal Aviation Administration closed all small airports for almost three months while officials contemplated whether to require bag searches, metal detectors, and other such security measures. In the end, noting the diversity in general aviation airports −− some are no more than dirt strips in a field while others, like New Jersey's Teterboro outside of New York City, are bigger than some commercial airports −− federal officials opted to allow each to come up with its own security measures. Meanwhile, the Transportation Security Administration has worked with the general aviation lobby to create an "Airport Watch" program, which is similar to the "Neighborhood Watch" anticrime initiative.
   Source: http://csmonitor.com/2005/0629/p03s02−usju.html

7. *June 29, Associated Press* — **Southwest to sell seats on ATA flights.** Southwest Airlines will sell seats on ATA Airlines connecting flights through Las Vegas to places such as Honolulu, Seattle and West Palm Beach, FL, beginning August 4. Under the code−sharing agreement announced Tuesday, June 28, Southwest and ATA will exchange passengers and luggage at Las Vegas McCarran Airport, with travelers able to buy a single ticket from either airline. The move by Dallas−based Southwest expands its partnership with ATA that began in February with connecting service in Chicago and was expanded Phoenix. Southwest estimates that it will get $50 million in additional revenue this year from selling tickets on ATA flights. Southwest Chief Executive Officer Gary Kelly said this month that ATA has approached Southwest about sharing international flights.
   Source: http://www.usatoday.com/travel/flights/2005−06−28−ata−southw est−codeshare_x.htm

8. *June 29, Auto Channel* — **AAA Chicago expects July 4th weekend travel to set record.** The roads and the skies will be the busiest ever for a Fourth of July holiday weekend, according to AAA Chicago. Roughly, 40.3 million Americans say they will travel 50 miles or more from home this weekend. That's 2.8 percent higher than last year. And, about 84 percent of travelers, or 33.9 million people, will travel by motor vehicle although the national average for regular unleaded gasoline is $2.21, which is a 30−cent increase from a year ago. "The biggest factor for this year's holiday increase is a three−day weekend," says Kris Lathan, AAA Chicago public affairs director. "This weekend follows the trend of increased travel throughout this year." This will be the most heavily traveled Fourth of July ever, and this long weekend will put more American travelers on the road than even the busiest holiday travel weekend −− Thanksgiving. Across the country, 4.6 million Americans will travel by plane, representing a 4.2 percent increase over last year. About five percent, or 1.8 million, of all holiday vacationers will travel by train, bus or other mode of transportation.
   Source: http://www.theautochannel.com/news/2005/06/29/136250.html

9. *June 29, Department of Transportation* — **Universities receive award grants for transportation education and research.** The Department of Transportation's Research and Innovative Technology Administration (RITA) on Wednesday, June 29, announced over $6.6

million in grants to be awarded to 10 University Transportation Centers (UTC) located throughout the United States for a variety of transportation education and research programs. Each school will receive $665,000 to support the full range of projects in their respective UTC programs. The schools receiving these grants are: University of Arkansas, University of California, University of Central Florida, University of Idaho, University of Missouri−Rolla, University of Southern California, University of Tennessee, North Dakota State University, Pennsylvania State University and San Jose State University. The diversity of the work being done at these specific UTCs is as varied as the geographic areas where the schools are located. For example, the University of Tennessee's UTC concentrates on transportation safety, while the University of Idaho's UTC specializes in advanced transportation technologies. More than 75 colleges and universities throughout the United States participate in the UTC program conducting transportation research, education and technology transfer. The UTC program is administered by RITA and grant recipients are required to provide matching funds.
More information on UTC grants can be found at http://www.rita.dot.gov.
Source: http://www.dot.gov/affairs/rita305.htm

10. *June 29, Transportation Security Administration* — **Summer Website for travelers.** The Transportation Security Administration (TSA) has launched a new Summer Traveler Website. Before traveling, the TSA encourages people to check the Summer Website and review the security screening procedures before going to the airport. Travelers can save themselves time at the airport if they take a few minutes to prepare. The TSA summer Website includes information that ranges from wait times at the security checkpoints to prohibited items to policies regarding food and beverages. It also has an area for Claims and Lost & Found items.
Summer Website: http://www.tsa.gov/interweb/assetlibrary/summerindex.htm
Source: http://www.tsa.gov/public/display?theme=40&content=090005198 013fe99

11. *May 27, Government Accountability Office* — **GAO−05−305: Combating Alien Smuggling: Opportunities Exist to Improve the Federal Response (Report).** Globally, alien smuggling generates billions of dollars in illicit revenues annually and poses a threat to the nation's security. Creation of the Department of Homeland Security (DHS) in March 2003 has provided an opportunity to use financial investigative techniques to combat alien smugglers by targeting and seizing their monetary assets. For instance, the composition of DHS's largest investigative component −− U.S. Immigration and Customs Enforcement (ICE) −− includes the legacy Customs Service, which has extensive experience with money laundering and other financial crimes. Another DHS component, U.S. Customs and Border Protection (CBP) has primary responsibility for interdictions between ports of entry. In summer 2003, ICE announced that it was developing a national strategy for combating alien smuggling. Among other objectives, the Government Accountability Office (GAO) determined the implementation status of the strategy and investigative results in terms of convictions and seized assets. To enhance the federal response to alien smuggling, GAO recommends that (1) the Secretary of Homeland Security establish a mechanism for tracking the results of referrals made by CBP to ICE and (2) the Attorney General consider developing and submitting to Congress a legislative proposal, with appropriate justification, for amending the civil forfeiture authority for alien smuggling. The departments agreed.
Highlights: http://www.gao.gov/highlights/d05305high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−305

[Return to top]

Postal and Shipping Sector

12. *June 29, DM News* — **Postal service, union reach tentative contract deal.** The U.S. Postal Service (USPS) and the American Postal Workers Union (APWU) reached a tentative one−year contract extension, the USPS said Tuesday, June 28. The agreement, if ratified by union members, will affect about 287,000 postal employees represented by the APWU. The tentative extension covers the period from November 20, 2005, through November 20, 2006. The tentative agreement provides for a 1.6 percent wage increase effective March 18, 2006, and includes the continuation of the cost−of−living allowance.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3322 8

13. *June 29, Rocky Mountain News (CO)* — **Colorado mail center receives detection system.** Postal officials Tuesday, June 28, unveiled the Colorado Springs' regional mail center's biohazard detection system. The new detection system is scheduled to be up and running next week. It will use a vacuum hood, air filters, and purified water to constantly test the air for strains of anthrax DNA. Anthrax spores can be released into the air when a contaminated envelope is compressed by mail−processing machinery, said distribution operations manager Walt Gale. The center's 468 employees process an average of 1.6 million pieces of mail per day and service more than 180 post offices across southern and central Colorado. More than 125 mail centers have the system. Nationally, 282 other mail processing sites are scheduled to install the system by the end of this year.
Source: http://rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_3890022,00.html

[Return to top]

Agriculture Sector

14. *June 29, Asahi Shimbun (Japan)* — **Five other chicken farms in Japan hit by avian flu.** Chickens at five farms near the one recently hit by the bird flu virus in Ibaraki Prefecture showed signs they had also been infected with the disease, the agricultural ministry said Tuesday, June 28. The five farms are located near the area in Mitsukaido where a diluted strain of avian flu virus was confirmed. The birds at the five farms were found carrying the antibody to the disease, indicating the birds had been infected with the virus. The ministry panel on poultry disease will study Wednesday, June 29, the necessity of destroying the chickens raised at the five farms. Government workers are in the process of culling 25,000 chickens at the infected farm in Mitsukaido.
Source: http://www.asahi.com/english/Herald−asahi/TKY200506290185.ht ml

[Return to top]

Food Sector

15.

June 29, Reuters — **Indonesia bans U.S. beef.** Indonesia will ban imports of U.S. beef and beef products from Thursday, June 30, due to concerns over bovine spongiform encephalopathy (BSE), or mad cow disease, a government official said. The U.S. on Friday, June 24, confirmed a second case of the brain−wasting mad cow disease in the U.S. herd, in a beef cow at least eight−year−old. Last year, Indonesia joined more than a dozen countries in banning U.S. beef after a first case of the disease was discovered in a Washington state dairy cow. Jakarta lifted that ban in May 2004. The ban, which will be for an indefinite period, will affect imports of live cows, meat, innards, and meat bone meal, but would not cover imports under permits granted before June 30, where delivery was due before or on August 30.
Source: http://www.reuters.com/newsArticle.jhtml?type=businessNews&s toryID=8922442

[Return to top]

Water Sector

16. *June 26, State (SC)* — **South Carolina: small water systems often have big problems.** Community water systems have been penalized more than twice as many times as government−owned systems for failing to obey safe drinking−water laws in South Carolina since the early 1990s, state records show. More than 300 small, privately owned residential water, and sewer systems dot the state's landscape, serving anywhere from a few dozen to a few thousand homes. The water systems often serve trailer parks and subdivisions built far from municipal water and sewer lines decades ago. And they are failing. The South Carolina Department of Health and Environmental Control (DHEC) issued more than 250 enforcement orders against the small, privately owned water systems −− with fines totaling more than $600,000 −− over the past 14 years. By comparison, the state sanctioned city, county, state and federal water systems slightly more than 100 times, levying $150,000 in fines, since 1991, according to DHEC records. Since the early 1970s, South Carolina has eliminated more than 400 small sewer plants that threatened water quality. Still, the state has as many as 200 additional plants, operated by various small, private utilities, that should be phased out, state officials say. Small, private water systems continue to provide service to about 81,000 of the state's four million residents, according to the agency's drinking−water protection division.
Source: http://www.thestate.com/mld/thestate/news/local/11988134.htm

[Return to top]

Public Health Sector

17. *June 29, Agence France Presse* — **Singapore starts preparing for bird flu pandemic.** Singapore has begun preparing for an Asian bird flu pandemic with influenza drugs already being stockpiled and joint ventures under way to develop a vaccine. The Health Ministry said warnings from the World Health Organization (WHO) about the bird flu mutating into a deadly, highly contagious human−to−human strain had prompted authorities in Singapore to heighten the alert. The ministry emphasized there was not yet any evidence the H5N1 virus, which has killed 38 Vietnamese, 12 Thais and four Cambodians since the beginning of the epidemic in 2003, was capable of human−to−human transmission. But it said a bird flu pandemic could be far more deadly and contagious than the Severe Acute Respiratory Syndrome (SARS), which

killed 33 people in Singapore and nearly 800 people globally in 2003. Under one pandemic scenario presented to the media, 550,000 people, or about a quarter of Singapore's population, would become infected in the first wave, resulting in more than 1,800 deaths. The ministry said that, although there was no vaccine available yet for the H5N1 strain of the virus, it had already begun buying Tamiflu, a drug currently used for the treatment of the type A influenza.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050629/hl_afp/healthflusingapore_050629113121

18. *June 29, Associated Press* — **Vietnam to begin mass vaccination of poultry in August to combat bird flu.** Vietnam announced Wednesday, June 29, it will begin vaccinating poultry nationwide against bird flu in August amid concerns that the disease could mutate and spread among humans, sparking a global pandemic. Starting August 1, commercial poultry operations and smaller household farms in northern Nam Dinh province and southern Tien Giang province in the Mekong Delta will be vaccinated, said Bui Quang Anh, head of Vietnam's animal health department. Vaccinations will be slowly expanded to another 40 high−risk provinces over the next two years, he said. Bird flu began ravaging poultry farms across Vietnam in late 2003, killing or forcing the slaughter of more than 45 million birds. The virus began jumping to humans at about the same time, and has killed 38 people in Vietnam, 12 in Thailand, and four from Cambodia. A team of virologists and epidemiologists from Hong Kong, Japan, Britain, and the United States in Vietnam last week discovered no changes in the virus' form, according to the World Health Organization (WHO), which coordinated their visit. The two−year poultry vaccination program will cost a total of $35 million, with the government subsidizing $29 million of the costs.
Source: http://asia.news.yahoo.com/050629/ap/d8b19ve00.html

19. *June 29, Agence France Presse* — **Top scientists downgrade risk of imminent bird flu pandemic.** International scientists have downgraded the risk of an imminent bird flu pandemic, hailing as "very good news" indications that the virus has not mutated, the World Health Organization (WHO) said. A team of virologists and epidemiologists from Britain, Hong Kong, Japan, and the United States left Vietnam Tuesday, June 28, after judging that the threat posed by the H5N1 strain to humans is lower than previously thought. The organization said last year that millions of people could die if the avian virus mutated to become easily transmissible between humans and caused a global pandemic. "The most important thing is that we could rule out that there was an immediate, imminent pandemic," stated Hans Troedsson, WHO representative in Vietnam. The team concluded that preliminary data does not suggest any increase in the efficiency of the disease's transmission either from birds to humans or from humans to humans. Troedsson also said the experts were also unable to confirm suggestions that a number of people might have been infected without showing symptoms. While the team's findings are good news, Hitoshi Oshitani, team leader and WHO's regional advisor on Communicable Disease Surveillance and Response, asked the international community to stay on guard.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050629/hl_afp/healthfluvietnam_050629134755

20. *June 29, Duluth Superior (MN)* — **Plans to test anthrax shot on children questioned.** The government's effort to develop a new vaccine against anthrax has raised red flags among critics over plans to eventually test an experimental version on children. Robert Bock, a spokesperson

for the National Institute of Child Health and Human Development, said the new anthrax vaccine would not be tested on 100 first− and second−graders until it is first tested safely on adults. While federal rules govern how children can be used in medical research, Barbara Loe Fisher, president of the National Vaccine Information Center, said the threat of anthrax exposure was too remote to subject children to a possibly dangerous substance. "The benefits are zero and risk is quite high," she states. Several pediatricians involved in bioterrorism issues, however, said that given the potential threat, it would be irresponsible not to include children in the test. "Considering that in a worst−case scenario, this vaccine would have to be used in an emergency over a very short period of time, we would be in a bad position medically and ethically if it were not tested beforehand," said Stanley Plotkin, emeritus professor of pediatrics at the University of Pennsylvania.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/politi cs/12012556.htm

21. *June 29, KLTV 7 (TX)* — **Texas man contracts disease associated with livestock.** Amarillo, TX, State health officials are looking into how a man contracted a rare bacterial disease typically tied to the livestock industry. The Texas Department of State Health Services says the Moore County, TX man doesn't work around livestock or in a laboratory or slaughterhouse. Department veterinarian James Alexander also says the man isn't a veterinarian, but that it's possible the man might have caught the disease from contaminated soil. Alexander says the disease can spread from animals to humans and the patient says he has a friend with livestock, but that he had no contact with the animals. Common symptoms resemble a serious case of the flu−sudden high fever, chills, sweats, a general feeling of sickness and loss of appetite. Blood tests are used to test for Q fever, and how it responds to antibiotics. Patients usually recover promptly when treatment is started without delay. The disease is caused by a bacteria known as Coxiella burnetii that is primarily carried by cattle, sheep and goats.
Source: http://www.kltv.com/Global/story.asp?S=3536399

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *June 29, Los Alamos Monitor (NM)* — **Canine trainers help rescuers.** An all−volunteer search and rescue (SAR) team and their canine companions stand ready to respond to any emergency in the mountains around Los Alamos, NM. Mountain Canine Corps (MCC) members, made up of citizens and dogs from throughout the community, sharpen their skills during weekly training in SAR missions in the wilderness around Los Alamos. MCC is a nonprofit search and rescue organization. Their mission is the training and fielding of search dogs and personnel to help locate missing persons. MCC is a member of the New Mexico Emergency Services Council and the National Association for Search and Rescue. They are called out for searches, often along with many other teams, through the Incident Command System (ICS). The state police initiate all SAR missions in New Mexico. As a SAR team, a

variety of training outside of dog and scent theory training is crucial for the members in order for them to contribute to missions in a safe and meaningful way. The team also trains in navigation, map and compass, wilderness medicine, crime scene preservation, amateur radio, and man tracking. MCC has 15 licensed HAM radio operators, five certified Wilderness First Responders, and many Wilderness Advanced First Aid Certificated members.
Source: http://www.lamonitor.com/articles/2005/06/28/headline_news/n ews01.txt

23. *June 29, Houston Chronicle (TX)* — **Drill lets authorities ponder evacuation policies and evaluate escape routes.** "Hurricane Greg" was center stage during a daylong hurricane evacuation drill for 40 emergency management coordinators, law enforcement and state and federal officials in Houston, TX, on Tuesday, June 28. The drill, which included a terrorist threat to hurricane shelters, marked a continuing effort to prepare the region in case of a hurricane. Harris County Judge Robert Eckels, who also serves as the county's director of emergency management, said Tuesday's drill was aimed at implementing designated evacuation routes and deciding whether a mandatory evacuation−−a new tool given local authorities−−should be issued. Another detail for emergency personnel to consider is the evacuation of special needs residents, Eckels said. As demonstrated throughout the day, the group huddled to discuss and offer solutions.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/324541 6

24. *June 28, Government Executive* — **FBI launches regional data sharing system.** The FBI is rolling out a program that allows federal law enforcement agencies and state and local police forces to share information throughout local regions of the country. The Regional Data Exchange works through local law enforcement offices and allows state, local and tribal law enforcement investigators access to federal information and intelligence data relevant to investigations within their jurisdictions. The program was first launched in St. Louis as part of the FBI's National Information Sharing System, and a similar program will be established in Seattle later this summer. Plans for augmenting the system include adding data from the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Marshals Service and the Federal Bureau of Prisons. The Seattle program will link with the Naval Criminal Investigative Service's Law Enforcement Information Exchange, which serves as the region's law enforcement information−sharing system. Information on the system includes the identities of vehicles and weapons, addresses and phone numbers. The program allows cases to be plotted on maps so geographical patterns can be identified. Users are able to update data on their own and as often as necessary.
Source: http://www.govexec.com/dailyfed/0605/062805p1.htm

[Return to top]

Information Technology and Telecommunications Sector

25. *June 29, Government Accountability Office* — **GAO−05−845T: Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks (Testimony).** For its testimony, GAO was asked to discuss the findings and recommendations of its recent study of IPv6 (GAO−05−471). In this study, GAO was asked to (1) describe the key characteristics of IPv6; (2) identify the key planning considerations for federal agencies in transitioning from IPv4 to IPv6; and (3) determine the progress made by the Department of

Defense (DOD) and other major agencies in the transition to IPv6. DOD has made progress in developing a business case, policies, timelines, and processes for transitioning to IPv6. Unlike DOD, the majority of other major federal agencies reported that they have not yet initiated key planning efforts for IPv6. In its report, GAO recommended, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin to address key planning considerations for the IPv6 transition and that agencies act to mitigate near−term IPv6 security risks. Highlights: http://www.gao.gov/highlights/d05845thigh.pdf
Source: http://www.gao.gov/new.items/d05845t.pdf

26. *June 28, Secunia* — **CSV_DB / i_DB arbitrary command execution vulnerability.** A vulnerability has been reported in CSV_DB 1.0, which can be exploited by malicious people to execute arbitrary commands. Input passed to the "file" parameter in csv_db.cgi is not properly sanitized before being used. This can be exploited to execute arbitrary commands on the server by appending the commands to the end of the "file" parameter using the pipe character. The vendor has confirmed that the vulnerability also affects i_DB version 1.0.
Source: http://secunia.com/advisories/15842/

27. *June 28, FrSIRT* — **phpBB "viewtopic.php" remote PHP code execution vulnerability.** A vulnerability was identified in phpBB, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "viewtopic.php" script that does not properly filter the "highlight" parameter before calling the "preg_replace()" function, which may be exploited by remote attackers to execute arbitrary PHP commands with the privileges of the web server.
Solution: http://www.phpbb.com/downloads.php
Source: http://www.frsirt.com/english/advisories/2005/0904

28. *June 28, US−CERT* — **Scanning activity on port 445/tcp.** US−CERT has seen reports indicating an increase in scanning activity of port 445/tcp. This port is used by Server Message Block (SMB) to share files, printers, serial ports and communicate between computers in a Microsoft Windows environment. Scanning for port 445/tcp has been active for a number of years. In 2004, Microsoft released a bulletin (MS04−011) describing a vulnerability in the Local Security Authority Subsystem Service (LSASS). Since this time a number of exploits have been published that take advantage of this vulnerability. More recently, Microsoft published two security bulletins (MS05−011 and MS05−027) that describe vulnerabilities in the Server Message Block (SMB). The LSASS and SMB services utilize RPC for communications. Ports configured to support RPC (i.e., port 445/tcp) may be scanned to locate vulnerable hosts. Scanning for port 445/tcp could be a result of attempts to exploit any of the vulnerabilities referenced above or attempts to authenticate to Microsoft Windows systems through brute force password attacks. More recently, an exploit was released that attempts to take advantage of the vulnerability described in MS05−011. While reports of successful system compromises using this vulnerability have not been confirmed, US−CERT strongly recommends that users patch their systems as soon as possible.
Source: http://www.us−cert.gov/current/current_activity.html#smb

29. *June 28, eSecurity Planet* — **Security executives: under pressure and under prepared.** A new survey of corporate security executives shows that their jobs are more difficult to handle than just a year ago, and they're not prepared to handle some significant security issues. Nearly

100 percent of CSOs say they are well prepared to handle spam, malware, denial−of−service attacks, and hacker attacks, according to a survey by CSO Interchange at a conference held last week in Chicago, IL, for chief security officers. However, 88 percent say their organizations are least prepared to handle inadvertent loss of data, social engineering and inappropriate use. The survey also shows that sixty−four percent of CSOs are more concerned about compliance this year than they were last year, and 38 percent report their budget for compliance solutions grew during the past year; seventy−four percent say their organization must comply with more than five laws and regulations; sixty−eight percent say their security budget is less than 10 percent of their total IT budget; eighty−three percent outsource less than 10 percent of their security, and 40 percent do not outsource security processes at all, and seventy percent say they do not receive sufficient early warning for cyber attacks.
Survey results: http://www.csointerchange.org/docs/2005−06−24−chicago−pollin g−results.pdf
Source: http://www.esecurityplanet.com/trends/article.php/3516156

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports VERITAS has released security advisories disclosing vulnerabilities that affect multiple versions of Backup Exec for Windows and Netware Servers. Several components of Backup Exec are affected, including the Remote Agent, Server, NetBackup, Web Administration Console, and Admin Plus Pack Option. For more information, please see: http://www.us−cert.gov/current/current_activity.html The impact of the vulnerabilities ranges from Denial of Service (DoS) conditions to remote execution of arbitrary code. VERITAS has released patches to eliminate all of the reported issues. It is strongly recommended that administrators apply the patches immediately, as historically, vulnerabilities affecting Backup Exec have been targeted by attackers in a widespread fashion. * http://support.veritas.com/menu_ddProduct_BEWNT_view_ALERT.h tm Updated Port Status: Reports of increased activity on port 6101 have continued. Activity targeting TCP port 10000 has significantly increased since the release of the Metasploit Framework module. Administrators are strongly urged to apply the hotfixes as soon as possible. Strict filtering of TCP port 10000 and 6101 is also highly recommended. For specific hotfixes and udpates please review the following URLs: * http://seer.support.veritas.com/docs/276604.htm/a> * http://www.metasploit.org/projects/Framework/modules/exploit s/backupexec_agent.pm

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 27015 (halflife), 1026 (−−−), 135 (epmap), 139 (netbios−ssn), 6881 (bittorrent), 53 (domain), 80 (www), 32775 (sometimes−rpc13), 4672 (eMule)

	Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *June 29, Associated Press* — **Architects rethink Freedom Tower security.** On Wednesday, June 29, officials unveiled a more bomb−resistant design for the 1,776−foot Freedom Tower, which is to offer 2.6 million square feet of office space and is expected to become the world's tallest building. The latest design for the centerpiece of the former World Trade Center site calls for reinforcing the middle of the tower and topping it with a mast meant to evoke the Statue of Liberty's torch. After concerns were raised about security at the soaring skyscraper proposed as the centerpiece of the former World Trade Center site, architects went back to the drawing board. In an effort to make it more resistant to truck bombs, the building has been moved farther from West Street, a major North−South throughway along the west side of Manhattan. The distance from the street was increased from 25 to an average of 90 feet. The redesign is meant to signal a newly aggressive effort to rebuild the 16 acres devastated by the September 11, 2001, attack on the World Trade Center.
Source: http://www.usatoday.com/news/nation/2005−06−29−ny−freedomtow er_x.htm

31. *June 29, Knight Ridder−Tribune* — **Monument security in Washington, DC.** On September 7, 2004, the National Parks Service closed the 55 acres of land around the site of the Washington Monument for the construction of what it calls a "vehicle barrier security system" −− a barrier around the monument that protects it from potential attacks from a bomb−laden vehicle. When the $15 million effort is complete, officials hope interlocking concrete barricades will eliminate that threat, protecting one of the District’s most recognized landmarks. The monument was reopened to visitors April 1. Inside the outer security wall, construction crews unearth mounds of yellow dirt as they complete a face−lift to the grounds. Trees and grass will be planted. Bill Line, a spokesperson for the National Parks Service, says it should all be finished in time for July 4 festivities. July 4 is one of the summer's big draws, and the District board of tourism's Website says a crowd of nearly 300,000 people is expected. The Lincoln Memorial is also seeing improvements. Line says the park service is planning to construct security barriers around the memorial and also wants to improve the roads around it. Line says the project should be completed in August or September 2006.
Source: http://www.freep.com/features/travel/washington26e_20050626. htm

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer